

Notice of Allowability

Application No.

10/699,947

Examiner

Samson B. Lemma

Applicant(s)

JANARTHANAM ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment after final filed on 07/23/2007.
2. ☒ The allowed claim(s) is/are 1, 5, 7, 9 and 12.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

1. This is in reply to amendment after a final office action, filed **on July 23, 2007**.
Claims **2-4, 6, 8 and 10-11 have been canceled. Thus claims 1, 5, 7, 9 and 12 are pending/examined.**
2. There are now two independent claims, **namely 1 and 7.**

Allowable Subject Matter

3. **Claims 1, 5, 7, 9 and 12** are allowed.

Before the claims were amended, all limitation recited in the respective independent claims have been disclosed by the combination of **Admission and Ferrant**.

For instance referring to the independent claim 1 Admission discloses a method of testing a device [Title "testing the encryption function device" or see also on page 1, "DUT"/device under the test) comprising:

- **Providing a first data string [Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];**
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**
- **Encrypting the first data string [See figure 1, ref. "P1S1"] using an encryption algorithm [see page 2, lines 14-18, "AES"], to provide an encrypted data string; [Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];**
and
- **Comparing a characteristic of the encrypted data string with a characteristic of the second data string.[page 6, lines 14-19] (" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the**

Art Unit: 2132

matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical, because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.”)

- Admission does not explicitly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of “comparing a **characteristic of the encrypted data string with a characteristic of the second data string.**” [Column 1, lines 8-33] Furthermore **Ferrant** /secondary reference on the record that shows/ confirms that the expected value/second data string is stored in the memory structure before it is compared with the calculated value/first string. “A ROM including an array, each cell of which is accessible by means of a column address and of a row address, includes a **parity memory for storing the expected parity** of each row and of each column, an electrically programmable one-time programmable address memory, a testing circuit for, during a test phase, calculating the parity of each row and of each column, **comparing the calculated and expected parities** for each row and each column” [See abstract]

Art Unit: 2132

In the pervious office action, **claims 4, 11 and 12 have been found allowable**. Accordingly, independent claim 1 has been amended to include the limitations of dependent claims 2, 3 and 4. Claims 2 - 4 have been canceled. Independent claim 7 has been amended to include the limitations of dependent claims 8, 10 and 11. Claims 8, 10 and 11 have been canceled.

None of the prior art of record taken singularly or in combination teaches the amended independent claim 1 and 7.

Therefore independent claims 1 and 7 are found to be novel and are allowed.

4. The dependent claims which are dependent on the above independent claims 1 and 7 being further limiting to the independent claim, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-


Art Unit: 2132

3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.
08/03/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100